What is claimed is:

1. A communication network, comprising:

(A) local communication links,

(B) a plurality of separately located central office switching systems interconnected via trunk circuits for selectively providing switched call connections between at least two of the local communication links,

(C) a signaling communication system including at least one signaling network element, said signaling communication system configured to provide two-way communications of control data messages between and among said cental office switching systems and said signaling network element, said signaling communication system interconnecting the central office switching systems and said signaling network element;

(D) a signaling gateway, separate from the central office switching systems and connected to said signaling communications system, said signaling gateway including an interface connected to a remote communications network and configured to exchange said control data messages between said remote communication network and said signaling communication system, and

(E) a signaling system security monitor, separate from the central office switching systems, said signaling system security monitor configured to determine if said control data messages are contextually proper.

2. The communications network according to claim 1 wherein said signaling system security monitor is configured to evaluate said control data messages to determine an effect of said control messages if acted upon by one of (i) said central office switching systems and (ii) said network element and, in response, determine if said control data messages are proper.

3. The communications network according to claim 1 wherein said signaling system security monitor is further configured to correlate messages associated with a call or transaction to ensure that a proper relationship exists between parameter values in the correlated messages.

4. The communications network according to claim 1 wherein said control data messages comprise ISUP messages.

5. The communications network according to claim 1 wherein said signaling system security monitor is configured to selectively communicate said ISUP messages between said signaling gateway and one of said central office switching systems in response to a determination that said ISUP messages are proper.

6. The communications network according to claim 1 wherein said signaling network element comprises a service control point (SCP) wherein said signaling system security

monitor is configured to evaluate said control data messages sent to and received from said SCP, and correlate said messages to determine that said messages are proper and to ensure that a proper relationship exists between said messages and between parameter values of said messages.

7. The communications network according to claim 1 wherein said control data messages comprise TCAP messages.

8. The communications network according to claim 1 wherein said signaling system security monitor is configured to maintain records of the contexts of existing calls and transactions, and evaluate whether monitored messages are appropriate to those contexts.

9. A communication network, comprising:

(A) local communication links,

(B) a plurality of separately located central office switching systems interconnected via trunk circuits for selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages,

(C) a signaling communication system for two-way communications of said control data messages between said cental office switching systems, said signaling communication system interconnecting the central office switching systems;

(D) a signaling gateway, separate from the central office switching systems and connected to said signaling communications system, said signaling gateway including an interface connected to a remote communications network and configured to exchange said control data messages between said remote communication network and said signaling communication system, and

(E) a signaling system security monitor, separate from the central office switching systems, said signaling system security monitor configured to determine if said control data messages are contextually proper.

10. The communications network according to claim 9 wherein said signaling system security monitor is configured to evaluate said control data messages and correlate said messages to determine that said messages are proper and to ensure that a proper relationship exists between said messages and between parameter values of said messages.

11. The communications network according to claim 9 wherein said signaling system security monitor is further configured to correlate messages associated with a call or transaction to ensure that a proper relationship exists between parameter values in the correlated messages.

12. The communications network according to claim 10 wherein said control data messages comprise ISUP messages.

13. The communications network according to claim 12 wherein said signaling system security monitor is configured to selectively communicate said ISUP messages between said signaling gateway and one of said central office switching systems in response to a determination that said ISUP messages are proper.

14. The communications network according to claim 10 further comprising a service control point (SCP) wherein said signaling system security monitor is configured to evaluate said control data messages sent to and received from said SCP, and correlate said messages to determine that said messages are proper and to ensure that a proper relationship exists between said messages and between parameter values of said messages.

15. The communications network according to claim 10 wherein said control data messages comprise TCAP messages.

16. The communications network according to claim 15 further comprising a service control point (SCP) wherein said signaling system security monitor is configured to selectively communicate said TCAP messages between said signaling gateway and SCP in response to a determination that said TCAP messages are proper.

17. The communications network according to claim 9 wherein said signaling system security monitor is configured to maintain records of the contexts of existing calls and transactions, and evaluate whether monitored messages are appropriate to those contexts.

18. The communications network according to claim 9 wherein said signaling system security monitor is configured to selectively enable and inhibit said signaling gateway from exchanging said control data messages between said remote communication network and said signaling communication system.

19. The communications network according to claim 9 wherein said signaling communication system includes a service control point (SCP) and said signaling system security monitor includes a memory storing states of said central office switching systems and said SCP, said processor additionally responsive to said states for determining if said control messages are proper.

20. The communications network according to claim 9 wherein said signaling system security monitor is configured to selectively modify said control messages in response to a determination of the propriety of said control messages.

21. The communications network according to claim 9 wherein said signaling gateway

includes a signaling protocol converter.

22. The communications network according to claim 21 wherein said signaling protocol converter is configured to convert SS7 type messages to another packet data format.

23. The communications network according to claim 22 wherein the other packet data format is an Internet Protocol (IP) format.

24. The communications network according to claim 21 wherein said signaling system security monitor is configured to monitor information contained in an MTP Layer 3 portion of said control data messages.

25. The communications network according to claim 24 wherein said information contained in said MTP Layer 3 portion of said control data messages includes (i) a destination point code, (ii) an originating point code, and (iii) a service indicator.

26. The communications network according to claim 9 wherein said signaling system security monitor is configured to monitor at least one of SCCP, ISUP, TCAP, and AIN messages.

27. The communications network according to claim 9 wherein said signaling system security monitor is configured to monitor a plurality of message types selected from

SCCP, ISUP, TCAP, and AIN type messages.

28. The communications network according to claim 9 wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in SCCP message portions of said control data messages.

29. The communications network according to claim 28 wherein said signaling system security monitor is configured to determine if said monitored calling and called party address parameters are consistent with an authorized signaling relationship.

30. The communications network according to claim 9 wherein said signaling system security monitor is configured to monitor calling and called party address parameters contained in an SCCP message portion of said control data messages.

31. The communications network according to claim 9 wherein said signaling system security monitor is configured to monitor origination and destination point codes contained in the MTP header of the control data messages and calling and called party address parameters contained in the SCCP message portion of said control data messages.

32. The communications network according to claim 9 wherein said signaling system security monitor is configured to monitor origination and destination point code parameters contained in the MTP header of said control data messages and determine if

a particular destination point code is authorized to send a particular message to a particular destination point code.

33. The communications network according to claim 9 wherein said signaling system security monitor includes a memory storing a state of said communications network.

34. The communication network according to claim 9 wherein said signaling system security monitor includes a memory storing permissible states of said communications network and rules for transitioning from each of said permissible states to others of said permissible states.

35. The communications network according to claim 9 wherein said signaling system security monitor includes a memory storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

36. The communications network according to claim 9 wherein said signaling system security monitor includes a memory storing data relating transaction status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

37. The communications network according to claim 9 wherein said signaling system

security monitor includes a memory storing a plurality of message templates.

38. The communications network according to claim 27 wherein said plurality of message templates are associated with a plurality of service providers.

39. The communications network according to claim 38 wherein said signaling system security monitor associates each of said control data messages with a corresponding one of said service providers and selects one of said message templates in response to the corresponding one of said service providers.

40. The communications network according to claim 9 wherein said signaling system security monitor includes a memory storing sets of templates, each of said sets corresponding to control messages appropriate to a particular call progress flow or transaction.

41. The communications network according to claim 40 wherein said templates define message formats, parameters and values associated with control message types selected from SCCP, ISUP, TCAP and AIN type messages.

42. The communications network according to claim 40 wherein said signaling system security monitor is configured to select said sets of templates in response to service provider authorization data associated with respective ones of said control data messages.

43. The communications network according to claim 9 wherein said signaling system security monitor comprises a certification agent configured to exchange and maintain encryption key certificates.

44. The communications network according to claim 9 wherein said signaling system security monitor is configured to issue and decrypt digital time stamps.

45. The communications network according to claim 9 wherein said signaling system security monitor comprises a digital certificate issuing authority.

46. The communications network according to claim 9 wherein said signaling system security monitor includes data encryption and decryption facilities.

47. A method of securely interfacing control links of respective communication networks, comprising the steps of:

exchanging control data messages between a remote communication network and a local signaling communication system;

interpreting said control data messages to determine whether it is appropriate with respect to a destination point code of said control data message and, in response, determining if said control data messages are proper;

selectively communicating control data messages between cental office switching systems; and

selectively providing switched call connections between at least two of the local communication links in response to predetermined control data messages.

48. The method according to claim 47 wherein said step of interpreting include steps of maintaining records of the contexts of existing calls and transactions, and evaluating whether monitored messages are appropriate to those contexts.

49. The method according to claim 47 wherein said signaling system wherein said step of selectively communicating control data messages includes selectively enabling and inhibiting said signaling gateway from exchanging said control data messages between said remote communication network and said signaling communication system.

50. The method according to claim 47 further including a step of storing states of respective ones of said central office switching systems, wherein said interpreting step is additionally responsive to said states for determining if said control messages are proper.

51. The method according to claim 47 further comprising a step of selectively modifying said control messages in response to a determination of an impropriety of said control messages.

52. The method according to claim 47 further comprising a step of converting a protocol of said control data messages between a protocol of said remote communication network and a protocol of said local signaling communication system.

53. The method according to claim 52 wherein one of said protocols is an SS7 compliant message protocol.

54. The method according to claim 52 wherein one of said protocols is an Internet Protocol (IP) format.

55. The method according to claim 52 wherein said signaling system security monitor is configured to monitor information contained in an MTP Layer 3 portion of said control data messages.

56. The method according to claim 55 wherein said information contained in said MTP Layer 3 portion of said control data messages includes (i) a destination point code, (ii) an originating point code, and (iii) a service indicator.

57. The method according to claim 47 wherein said interpreting step includes monitoring of at least one of SCCP, ISUP, TCAP, and AIN messages.

58. The method according to claim 47 wherein said interpreting step includes monitoring

of a plurality of message types selected from SCCP, ISUP, TCAP, and AIN type messages.

59. The method according to claim 47 wherein said interpreting step includes monitoring of calling and called party address parameters contained in SCCP message portions of said control data messages.

60. The method according to claim 47 wherein said interpreting step includes determining if said monitor calling and called party address parameters are consistent with an authorized signaling relationship.

61. The method according to claim 47 wherein said interpreting step includes monitoring calling and called party address parameters contained in an SCCP message portion of said control data messages.

62. The method according to claim 47 wherein said interpreting step includes monitoring origination and destination point codes contained in the MTP header of the control data message and calling and called party address parameters contained in the SCCP message portion of said control data messages.

63. The method according to claim 47 wherein said interpreting step includes monitoring origination and destination point codes parameters contained in the MTP header of said

control data messages and determining if a particular destination point code is authorized to send a particular message to a particular destination point code.

64. The method according to claim 47 further comprising a step of storing a state of said communications network.

65. The method according to claim 47 further comprising a step of storing (i) permissible states of said communications network and (ii) rules for transitioning from each of said permissible states to others of said permissible states.

66. The method according to claim 47 further comprising a step of storing data relating call progress status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

67. The method according to claim 47 further comprising a step of storing data relating transaction status with respective sets of control messages appropriate to initiate a next action consistent with a particular service.

68. The method according to claim 47 further comprising a step of storing a plurality of message templates.

69. The method according to claim 68 wherein said plurality of message templates are

associated with a plurality of service providers.

70. The method according to claim 69 further comprising steps of:
associating each of said control data messages with a corresponding one of said service providers; and
selecting one of said message templates in response to the corresponding one of said service providers.

71. The method according to claim 47 further comprising a step of storing sets of templates, each of said sets corresponding to control messages appropriate to particular call progress flow.

72. The method according to claim 71 wherein said templates define message formats, parameters and values associated with control message types selected from SCCP, ISUP, TCAP and AIN type messages.

73. The method according to claim 71 further comprising a step of selecting said sets of templates in response to service provider authorization data associated with respective ones of said control data messages.

74. The method according to claim 47 further comprising steps of exchanging and maintaining encryption key certificates.

75. The method according to claim 47 further comprising steps of issuing and decrypting digital time stamps.

76. The method according to claim 47 further comprising a step of issuing a digital certificate.